In the United States Patent and Trademark Office
Board of Patent Appeals and Interferences

Reply Brief

In re the Application of:

David Michael SHACKELFORD
Serial No. 09/409,617
Filed: October 1, 1999
Attorney Docket No. TU999029

METHOD, SYSTEM, AND PROGRAM FOR DISTRIBUTING SOFTWARE BETWEEN COMPUTER SYSTEMS

Submitted by:

Konrad, Raynes & Victor LLP
315 So. Beverly Dr., Ste. 210
Beverly Hills CA 90212
(310) 556-7983
(310) 556-7984 (fax)

This Reply Brief is submitted in response to the Examiner Answer dated August 30, 2006, in which the Examiner continued the rejection of all the claims as anticipated (35 U.S.C. §102) and obvious (35 U.S.C. §102) over cited art. Applicants traverse the Examiner's findings in the Examiner Answer and submit that all pending claims 1-40 are patentable over the cited art and in condition for allowance for the following reasons.

On pgs 1-11 of the Examiner Answer, the Examiner repeated the rejections from the Final Office Action dated Dec. 13, 2005 ("Final Office Action").

A. Claims 1, 2, 8-11, 16, 17, 21-24, 27, 28, and 34-40 are Patentable Over the Cited Davis

The Examiner maintained the rejection of claims 1, 2, 8-14, 16, 17, 21-28, 34-40 as anticipated (35 U.S.C. §102(b)) by Davis (U.S. Patent No. 5,473,692).

1. Claims 1, 16, and 27

In the Response to Argument, the Examiner cited col. 8, line 23 to col. 9, line 26 of Davis as teaching the requirements of claims 1, 16, and 27. (Examiner Answer, pgs. 11-12). Applicants traverse.

The Examiner likens the cited first node of Davis to the claimed second computer system that is requesting software and the cited second node of Davis to the claimed first computer system that determines whether the requesting second node is authorized to use the software. (Examiner Answer, pg. 11).

The cited Davis mentions that the first hardware agent (first node):

> generates a response message by encrypting the decrypted challenge message with the public key of the second hardware agent ("PUK2") and transmits the response message to the second hardware agent. Then, the second hardware agent decrypts the response with its private key ("PUK1") as previously determined through decryption of the previously transmitted manufacturer's device certificate (Step 245).

(Davis, col. 8, lines 52-60).

The claims require that the first computer system (likened to the second hardware agent) maintains keys of computer systems authorized to access the software and

determine whether there is one such maintained key for the second computer system (cited first hardware agent).

The cited Davis does not disclose this requirement because in the cited col. 8 the second hardware agent does not determine whether there is one maintained key for the first hardware agent to use to decrypt the response to the challenge as claimed. Instead, in the cited col. 8, the requesting first hardware agent encrypts the response to the challenge using the public key (PUK2) of the second hardware agent that the second hardware agent decrypts using its own private key (PUK1).

The cited col. 8 does not have the second hardware agent use a determined maintained key for the first hardware agent of authorized systems to decrypt the challenge to the response. Instead, in the cited Davis, the second hardware agent uses its own private key to decrypt the response to the challenge. Thus, in the cited col. 8 there is no need for the second hardware agent to determine whether there is a key maintained for the first hardware agent from the keys of authorized users because the second hardware agent uses its own private key.

In the Response, the Examiner also cited col. 5, lines 8-10 and 37-56 of Davis concerning additional protocols and found that this cited col. 5 discloses the claim requirement of determining whether there is one maintained key for the second computer system to decrypt the second computer system response to the message the first computer system sent to the second computer system. (Examiner Answer, pg. 12). Applicants traverse.

The cited col. 5, line 8 mentions that additional protocols are used to authenticate a message and legitimize the entity sending the message. The cited col. 5, lines 10-30 discusses authentication of the sender by incorporating a digital certificate issued by a mutually trusted authority. An original message 40 is encrypted with a symmetric key (SK) to form an encrypted message 65 that is input into the transmission message 50 along with the digital certificate 45. The original message 40 also undergoes a hash to form a transmitted message digest 75, which is further encrypted using the private key of the first node (PRK1) which is input into the transmission message 50. (Davis, col. 5, lines 32-45).

Of particular interest, is that Davis then mentions that the second node, upon receiving this message 50, decrypts the symmetric key (SK) with its private key and the digital certificate with a published key of the trusted authority to obtain the symmetric key (SK) 60 and the public key of the first node (PUK1 11). This first node public key (PUK1) is then used to decrypt the transmitted message (Davis, col. 5, lines 47-55).

Thus, in Davis the second node (likened to the claimed first computer system) obtains the public key of the first node (likened to the claimed requesting second computer system) by decrypting the transmission message from the first node. Nowhere does this cited col. 5 of Davis disclose that the second node (i.e., claimed first computer system) determine whether there is a key for the first node (claimed second computer system) from keys the second node maintains for computer systems authorized to access the software. Instead, Davis mentions that the cited second node obtains the first node public key by decrypting the transmission message from the first node, using in part a published public key (PUBTA) of a trusted authority.

Thus a careful examination of the specific decryption operations described in the cited col. 5 reveals that the cited col. 5 does not discloses a first computer system receiving a response sent by the second computer system (in response to a message from the first computer system) and determining whether one of the maintained keys of computers authorized to access the software is for the second computer system and capable of decrypting the received response. Further, nowhere does the cited Davis anywhere disclose that the first node is not authorized to access the software upon determining that there is no maintained key that can be used to decrypt the response from the first node (claimed second computer system).

Applicants further traverse certain of the Examiner's findings with respect to Davis.

For instance, the Examiner found that the "second node receives the public key of the first node from a trusted authority, and ultimately decrypts the encrypted message received from the first node", and that this finding satisfies the claim requirement of determining whether there is one maintained key for the second computer system. (Examiner Answer, pg. 12) Applicants traverse this finding.

First off, Davis does not say that the second node receives the public key (PUK1) of the first node from a trusted authority as the Examiner contends. Instead, Davis states "the second node 15 decrypts … the digital certificate 45 with a published key (PUBTA) of the trusted authority 55 to obtain … PUK1 11", which is the public key of the first node. (Davis, col. 5, lines 48-52) Thus, Davis does not say, as the Examiner contends, that the second node receives the public key (PUK1) of the first node from a trusted authority, but instead states that the second node use the published key of the trusted authority to decrypt the digital certificate 45 included in the message to obtain the first node public key. Thus, the cited Davis does not disclose determining whether one of a maintained keys is for the second computer system as claimed, but instead describes how the second node unwraps the public key of the first node using the PUBTA.

The Examiner further found that:

> Appellant's claims do not require the claimed first computer system to maintain a database of keys that are searched to find the key of the second computer system. Therefore the second node storing the public key of the first node for future processing meets the claimed maintaining.

(Examiner Answer, pgs. 12-13). Applicants traverse this finding.

The claims require that the first computer system maintain keys of computers authorized to access software and require that the first computer system determine whether one of these maintained keys is for the second computer system to use to decrypt the response from the second computer system. Applicants submit that the cited Davis teaches away from this requirement because in the cited col. 5 the second node does not maintain the public key of the first node with keys of systems authorized to access software, but instead obtains the public key of the first node when decrypting the message from the first node using a published public key of a trusted authority, not of systems authorized to access software as claimed.

Consequentially, the Examiner's contention that the "second node storing the public key of the first node for future processing meets the claimed maintaining" is incorrect because the claims require that this first node key be available before the message is decrypted in order to decrypt. The system of Davis is different than what is claimed because the first node key of Davis is not available prior to the decryption

described in col. 5, nor is the first node public key maintained by the second node as part of keys of systems authorized to access the software.

The Examiner further stated

> because the public key of the first node is being used to decrypt an encrypted message that was sent by the first node and encrypted with the private key of the first node, that public key of the first node would have been determined to be a maintained key for that first node that is capable of decrypted [sic] the received encrypted message.

(Examiner Answer, pg. 13). Applicants traverse this finding.

Although the second node of Davis uses the first node public key obtained from the transmitted message 50 to decrypt the received message, this still does not mean that the second node maintains the public key as part of "maintained keys" of systems authorized to access software.

The claims require that the key of the second computer systems be maintained for determining whether the requesting second system may access the software. The Examiner has not cited any part of Davis that discloses that the second node maintains the public key of the first node in order to determine whether the first node can access software as part of a request, message, response protocol as claimed. Instead, the cited col. 5 only describes that the second node obtains and uses the first node public key to decrypt a message from the first node, not to determine whether the first node may access the software to distribute. In fact, in the cited col. 5, the first node public key is obtained from the transmitted message while decrypting the message.

The Examiner further found that the preamble of claims 1, 16, and 17, concerning "distributing computer software from a first computer system" is not given patentable weight. (Examiner Answer, pgs. 13-14) However, the first and last limitations of these claims concern maintaining keys of systems authorized to access software and permitting the second computer system to access software after determining that the second computer system is authorized. Thus, the software authorization and access requirements cited as distinguishing factors are part of the claim limitations, not just the preamble as the Examiner contends.

The Examiner also found that Davis operates as the claims require because "[i]f the messages are not the same, communications are terminated, and no software access is

granted. Therefore, if the second node does not have the public key of the first node stored for decryption of the receiving message, communication with the first node will be terminated…. Such that the second computer system is not allowed to access software." (Examiner Answer, pg. 16).

Applicants traverse this finding because the cited col. 5 discusses a technique that is used to determine whether "communications are maintained between the legitimate nodes". (Davis, col. 5, lines 58-62). Once secure communication is established, the first hardware agent (or node) may request a license token from the second hardware agent. (Davis, col. 9, lines 2-25). Thus, in the cited Davis the second node uses the published key from the trusted authority to decrypt the message to obtain the first node public key in order to establish communication between the nodes, not to determine whether one node is authorized to access requested software.

The claims require that the response the first computer system decrypts using a maintained key for the second computer system is initiated in response to the second computer system requesting software. In the cited col. 5, the message exchange is used to establish communication and is not initiated in a response to a request for software as claimed.

Applicants further submit that additional Examiner arguments on pgs. 14-17 are addressed by the above explanations as to why the cited Davis does not disclose the claim requirements.

Accordingly, for all the above reasons, Applicants submit that claims 1, 16, and 17 are patentable over the cited Davis.

Claims 2, 8, 17, 21, 28, 34, 38-40 are patentable over the cited art because they depend from one of claims 1, 16, and 27.

2. Claims 12-14, 25, and 26

In the Response to Arguments, the Examiner stated that claims 12 and 25 do not contain the claimed requirement of determining whether there is one maintained key for the second computer system. (Examiner Answer, pg. 13) Notwithstanding, Applicants argued patentability of these claims in the Appeal Brief based on the requirements of claims 12 and 25, not limitations not found in the claims as the Examiner implies.

With respect to these claims, the Examiner argued that the distinction that the cited Davis does not disclose that the first hardware agent (corresponding to the claimed second computer system) encrypts the challenge message that can be decrypted with a key the first hardware agent provided to the second hardware agent (corresponding to the claimed first computer system) "is not persuasive because the claims do not require that the key, used to decrypt the encrypted message, be transmitted directly from the claimed second computer system to the claimed first computer system" (Examiner Answer, pg. 17).

Applicants traverse this finding because the first limitation of these claims specifically require the second computer system "providing a key to the first computer system capable of decrypting an encrypted response from the second computer system".

Applicants submit that the other distinctions Applicants made in the Appeal Brief with respect to claims 12 and 25 and Davis not addressed in the Examiner Answer still stand. For instance, as discussed, the challenge/response procedure of the cited col. 8 of Davis is for the purpose of ensuring secure communications between the hardware agents. The claims require that the second computer system receives access to the software in response to the encrypted response message. Nowhere does this cited col. 8 disclose that one agent receive access to requested software in response to the cited challenge/response procedure.

3. Claims 9, 22, and 35

With respect to these claims, the Examiner responded that the Applicants argument that nowhere does the cited Davis disclose that the second hardware agent maintain public keys from multiple authorized first hardware agents to use to decrypt their challenge response "is not persuasive because the background of Davis (col. 1, lines 40-49) shows that Davis is concerned with authorized multiple nodes to access software." (Examiner Answer, pgs. 17-18)

Applicants traverse this reasoning because even if Davis is concerned with multiple nodes accessing software, the Examiner still has not cited any part of Davis that discloses that the second hardware agent (claimed first computer system) maintains public keys from authorized computer systems that are used to decrypt a response part of

a request-message-response exchange initiated by the second computer system to access the software.

Accordingly, claims 9, 22, and 35 are patentable over the cited art.

4. Claims 10, 11, 23, 24, 36, and 37

In the Response, the Examiner found that the arguments were "not persuasive because the claims require the request for configuration data to come from the claimed second computer system (which correlates to the first node in Davis)." (Examiner Answer, pg. 18)

Applicants traverse this finding because the base claims in fact require that the message is generated by the first computer system. Thus, the requirement that the generated message includes a random component and a request for configuration information would "come from" the first computer system because, according to the claims, the first computer system generates this message.

The Examiner then explained on page 18 that the first node of Davis transmits a message having a certificate and the second node responds. Notwithstanding, the Examiner has not cited any part of Davis that discloses that the cited second node include a request for configuration data from the first node when responding to the first node's request.

Accordingly, Applicants request reversal of the rejection of claims 10, 23, and 36 on the grounds that the additional requirements of these claims are not disclosed in the cited Davis, thus providing additional grounds of patentability over the cited art.

B. Claims 3-7, 15, 18-20, and 29-33 are Patentable Over the Combination of References

The Examiner rejected claims 3-7, 15, 18-20, and 29-33 as obvious (35 U.S.C. §103) over Davis in view of different combinations of additional references.

In the Response, the Examiner dismissed Applicants arguments in the Appeal Brief on the grounds that Applicants argued the references individually and that one cannot show nonobviousness by attacking references individually. (Examiner Answer, pg. 18) Applicants traverse.

With respect to the obviousness rejections of claims 5, 6, 31, and 32, Applicants explained why the cited sections of Komura did not teach the additional requirements for which it was cited to address the shortcomings of Davis the Examiner acknowledged. Applicants submit that by showing that Komura fails to teach or suggest the limitations the Examiner acknowledged were not taught in the cited Davis, Applicants have explained why the cited combination of references does not teach or suggest the additional requirements of these dependent claims.

Moreover, with respect to claims 5, 6, 31, and 32, Applicants were not arguing references "individually" as the examiner contends because Applicants have shown why the cited art fails to teach the requirements for which it was cited.

Accordingly, Applicants submit that the additional requirements of these claims provide further grounds of patentability over the cited art.

Respectfully submitted,

/David Victor/

David W. Victor
Reg. No. 39,867

Dated: October 30, 2006

Direct All Correspondence to:
David Victor
Konrad Raynes & Victor LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, California 90212
Tel: 310-553-7977
Fax: 310-556-7984